(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－184314
（P2001－184314A）
(43)公開日　平成13年７月６日(2001.7.6)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｚ	５Ｂ０１７
	12/00	５４５	12/00	５４５Ｍ	５Ｂ０４９
	12/14	３２０	12/14	３２０Ｂ	５Ｂ０８２
	13/00	３５４	13/00	３５４Ｚ	５Ｂ０８５
	17/60	ＺＥＣ	15/21	ＺＥＣＺ	５Ｂ０８９

審査請求　未請求　請求項の数12　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平11－370556

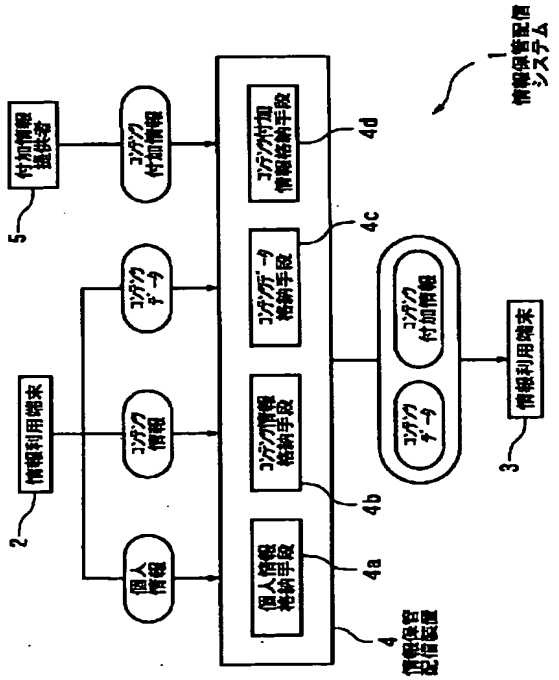
(22)出願日　平成11年12月27日(1999.12.27)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　永井　規浩
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100092152
弁理士　服部　毅巖

最終頁に続く

(54)【発明の名称】　情報利用端末、情報保管配信装置、情報保管配信システム及び記録媒体

(57)【要約】
【課題】　使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行う。
【解決手段】　利用者が使用権を取得したコンテンツを、情報利用端末２を用いて情報保管配信装置４に送信し、情報保管配信装置４は、そのコンテンツを保管し、利用者が情報保管配信装置４に格納されたコンテンツの利用を希望する場合、利用者は情報利用端末３を用いて情報保管配信装置４に格納されたコンテンツの配信を要求し、情報保管配信装置４は、要求されたコンテンツをコンテンツ付加情報とともに情報利用端末３に配信する。



1

【特許請求の範囲】

【請求項１】　コンテンツデータの利用を行う情報利用端末において、

前記コンテンツデータの保管及び配信を行う情報保管配信装置に送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、

前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、

端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、

前記情報保管配信装置との認証処理を行い、前記情報保管配信装置との共有鍵であるセッション鍵を生成する認証手段と、

前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、

前記コンテンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を前記情報保管配信装置に送信する情報送信手段と、

を有することを特徴とする情報利用端末。

【請求項２】　配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、

前記配信コンテンツ選択手段による選択に応じて抽出され、前記コンテンツ鍵によって暗号化された前記コンテンツデータ、前記端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、

前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、

前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、

前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段と、

をさらに有することを特徴とする請求項１記載の情報利用端末。

【請求項３】　前記セッション鍵により暗号化され、前記情報保管配信装置から送信されたコンテンツリストを受信するコンテンツリスト受信手段と、

前記コンテンツリスト受信手段によって受信された前記コンテンツリストを前記セッション鍵により復号するコンテンツリスト復号手段と、

をさらに有することを特徴とする請求項２記載の情報利用端末。

2

【請求項４】　コンテンツデータの利用を行う情報利用端末において、

前記コンテンツデータの保管及び配信を行う情報保管配信装置との認証処理を行い、前記情報保管配信装置との共有鍵であるセッション鍵を生成する認証手段と、

配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、

前記配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、

前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、

前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、

前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段と、

を有することを特徴とする情報利用端末。

【請求項５】　前記セッション鍵により暗号化され、前記情報保管配信装置から送信されたコンテンツリストを受信するコンテンツリスト受信手段と、

前記コンテンツリスト受信手段によって受信された前記コンテンツリストを前記セッション鍵により復号するコンテンツリスト復号手段と、

をさらに有することを特徴とする請求項４記載の情報利用端末。

【請求項６】　コンテンツデータの保管及び配信を行う情報保管配信装置において、

前記コンテンツデータの利用を行う情報利用端末との認証処理を行い、前記情報利用端末との共有鍵であるセッション鍵を生成する認証手段と、

コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を受信する情報受信手段と、

前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、

センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、

前記情報受信手段によって受信された前記コンテンツデータ、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格

納手段と、
前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、
利用者の個人情報を格納する個人情報格納手段と、
付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、
前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、
前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、
コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、
前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、
前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信する情報配信手段と、
を有することを特徴とする情報保管配信装置。

【請求項７】　前記コンテンツ付加情報抽出手段は、前記個人情報及び前記コンテンツ情報に基づいて、前記コンテンツ付加情報の抽出を行うことを特徴とする請求項６記載の情報保管配信装置。

【請求項８】　前記コンテンツデータ格納手段に格納された前記コンテンツデータのリストであるコンテンツリストを作成するコンテンツリスト作成手段と、
前記コンテンツリスト作成手段によって作成された前記コンテンツリストを前記セッション鍵により暗号化するコンテンツリスト暗号化手段と、
前記コンテンツリスト暗号化手段によって暗号化された前記コンテンツリストを前記情報利用端末に送信するコンテンツリスト送信手段と、
をさらに有することを特徴とする請求項６記載の情報保管配信装置。

【請求項９】　コンテンツデータの保管及び配信を行う情報保管配信システムにおいて、
送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、認証処理を行い、共有鍵であるセッション鍵を生成する認証手段と、前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、前記コンテンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する情報送信手段とを有する情報利用端末と、
配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、前記配信コンテンツ選択手段による選択に応じて抽出され、前記コンテンツ鍵によって暗号化された前記コンテンツデータ、前記端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段とを有する情報利用端末と、
前記情報利用端末との認証処理を行い、前記セッション鍵を生成する認証手段と、前記情報利用端末から送信された前記コンテンツデータ、前記コンテンツ鍵、及び前記コンテンツ情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、前記情報受信手段によって受信された前記コンテンツデータ、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格納手段と、前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、利用者の個人情報を格納する個人情報格納手段と、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信

する情報配信手段とを有する情報保管配信装置と、
を有することを特徴とする情報保管配信システム。
【請求項１０】　送信するコンテンツデータの選択を行い、
選択された前記コンテンツデータをコンテンツ鍵によって暗号化し、
端末秘密鍵によって前記コンテンツ鍵を暗号化し、
認証処理を行い、共有鍵であるセッション鍵を生成し、
暗号化された前記コンテンツ鍵を前記セッション鍵により暗号化し、
暗号化された前記コンテンツデータ、前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する機能をコンピュータに行わせるプログラムを格納する記録媒体。
【請求項１１】　認証処理を行い、共有鍵であるセッション鍵を生成し、
配信を希望するコンテンツの選択を行い、
利用者の選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信し、
受信された前記コンテンツ鍵及び前記コンテンツ付加情報を前記セッション鍵により復号し、
前記セッション鍵によって復号された前記コンテンツ鍵を前記端末秘密鍵により復号し、
復号された前記コンテンツ鍵により、前記コンテンツデータを復号する機能をコンピュータに行わせるプログラムを格納する記録媒体。
【請求項１２】　認証処理を行い、共有鍵であるセッション鍵を生成し、
コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を受信し、
前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号し、
センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化し、
受信した前記コンテンツデータ、及び暗号化された前記コンテンツ鍵を格納し、
受信した前記コンテンツ情報を格納し、
利用者の個人情報を格納し、
付加情報提供者が提供するコンテンツ付加情報を格納し、
各利用者に応じた前記コンテンツ付加情報を抽出し、
利用者に選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出し、
抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号し、
復号された前記コンテンツ鍵、及び抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化し、
抽出された前記コンテンツデータ、及び暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を配信する機能をコンピュータに行わせるプログラムを格納した記録媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツデータの利用を行う情報利用端末、コンテンツデータの保管及び配信を行う情報保管配信装置、情報保管配信システム、及びそれらの機能をコンピュータに行わせるプログラムを格納した記録媒体に関し、特に、通信ネットワークを利用した情報利用端末、情報保管配信装置、情報保管配信システム、及びそれらの機能をコンピュータに行わせるプログラムを格納した記録媒体に関する。
【０００２】
【従来の技術】従来、音楽、映像等のコンテンツの使用権取得は、ＣＤ、ＤＶＤ等のコンテンツデータが格納された記録媒体を購入するか、インターネット等の電子通信回線を通じ、コンテンツデータをダウンロードすることによって行われてきた。電子通信回線を通じてダウンロードしたコンテンツデータは、その電子通信回線に接続されたコンピュータ等が有するハードディスク等の記録装置、或いはメモリースティック、フロッピーディスク、ＭＤ等の記録媒体に格納され、利用者は、それらに格納されたコンテンツを再生することにより、取得したコンテンツの利用を行うことができる。
【０００３】
【発明が解決しようとする課題】しかし、ダウンロードしたコンテンツデータを記録装置に格納する方法では、記録装置が有する記憶容量を上限として、保有できるコンテンツが制限されてしまうという問題点がある。
【０００４】また、ＣＤ等の記録媒体を入手する方法、及びダウンロードしたコンテンツデータを記録媒体に格納する方法では、利用者は、コンテンツデータを格納した記録媒体を別途保管しておかなければならないため、管理上の利便性に欠け、コンテンツ再生時におけるコンテンツの選択が困難であるという問題点がある。
【０００５】さらに、コンテンツデータを格納した記録媒体を用いる場合、この記録媒体を所持していない場合においては、コンテンツの再生を行うことができないという問題点もある。
【０００６】また、コンテンツデータを格納した記録媒体を用いる場合、コンテンツを再生する情報利用装置にはこの記録媒体の収納部及び駆動部が必要となり、情報利用装置の小型化が図れないという問題点もある。
【０００７】さらに、従来の方法では、取得したコンテンツに関する最新情報等の入手は、利用者が別途に行わ

なければならないという問題点がある。本発明はこのような点に鑑みてなされたものであり、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、装置の小型化を図り、利用者に適した各種情報の提供を行うことが可能な情報利用端末を提供することを目的とする。

【０００８】また、本発明の他の目的は、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能な情報保管配信装置を提供することである。

【０００９】さらに、本発明の他の目的は、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能な情報保管配信システムを提供することである。

【００１０】また、本発明の他の目的は、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下であってもコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者へ利用者に適した各種情報の提供を可能とする機能をコンピュータに行わせるプログラムを格納した記録媒体を提供することである。

【００１１】

【課題を解決するための手段】本発明では上記課題を解決するために、コンテンツデータの利用を行う情報利用端末において、前記コンテンツデータの保管及び配信を行う情報保管配信装置に送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、前記情報保管配信装置との認証処理を行い、前記情報保管配信装置との共有鍵であるセッション鍵を生成する認証手段と、前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、前記コンテンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を前記情報保管配信装置に送信する情報送信手段とを有することを特徴とする情報利用端末が提供される。

【００１２】ここで、送信コンテンツ選択手段は、情報保管配信装置に送信するコンテンツデータの選択を行い、コンテンツ鍵暗号化手段は、送信コンテンツ選択手段によって選択されたコンテンツデータをコンテンツ鍵によって暗号化し、端末秘密鍵暗号化手段は、端末秘密鍵によってコンテンツ鍵を暗号化し、認証手段は、情報保管配信装置との認証処理を行い、情報保管配信装置との共有鍵であるセッション鍵を生成し、セッション鍵暗号化手段は、端末秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を、セッション鍵により暗号化し、情報送信手段は、コンテンツ鍵暗号化手段によって暗号化されたコンテンツデータ、セッション鍵暗号化手段によって暗号化されたコンテンツ鍵、及びコンテンツデータの内容を示すコンテンツ情報を情報保管配信装置に送信する。

【００１３】また、コンテンツデータの利用を行う情報利用端末において、前記コンテンツデータの保管及び配信を行う情報保管配信装置との認証処理を行い、前記情報保管配信装置との共有鍵であるセッション鍵を生成する認証手段と、配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、前記配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段とを有することを特徴とする情報利用端末が提供される。

【００１４】ここで、認証手段は、情報保管配信装置との認証処理を行い、情報保管配信装置との共有鍵であるセッション鍵を生成し、配信コンテンツ選択手段は、配信を希望するコンテンツの選択を行い、情報受信手段は、配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵により暗号化されたコンテンツ鍵、及びセッション鍵によって暗号化されたコンテンツ付加情報を受信し、セッション鍵復号手段は、情報受信手段によって受信されたコンテンツ鍵及びコンテンツ付加情報をセッション鍵により復号し、端末秘密鍵復号手段は、セッション鍵によって復号されたコンテンツ鍵を端末秘密鍵により復号し、コンテンツ鍵復号手段は、端末秘密鍵復号手段によって復号されたコンテンツ鍵によりコンテンツデータを

復号する。

【００１５】さらに、コンテンツデータの保管及び配信を行う情報保管配信装置において、前記コンテンツデータの利用を行う情報利用端末との認証処理を行い、前記情報利用端末との共有鍵であるセッション鍵を生成する認証手段と、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、前記情報受信手段によって受信された前記コンテンツデータ、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格納手段と、前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、利用者の個人情報を格納する個人情報格納手段と、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信する情報配信手段とを有することを特徴とする情報保管配信装置が提供される。

【００１６】ここで、認証手段は、情報利用端末との認証処理を行い、情報利用端末との共有鍵であるセッション鍵を生成し、情報受信手段は、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵によって暗号化されたコンテンツ鍵、及びコンテンツデータの内容を示すコンテンツ情報を受信し、セッション鍵復号手段は、情報受信手段によって受信されたコンテンツ鍵をセッション鍵により復号し、センタ秘密鍵暗号化手段は、セッション鍵復号手段によりコンテンツデータ格納手段は、情報受信手段によって受信されたコンテンツデータ、及びセンタ秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を

格納し、コンテンツ情報格納手段は、情報受信手段によって受信されたコンテンツ情報を格納し、個人情報格納手段は、利用者の個人情報を格納し、コンテンツ付加情報格納手段は、付加情報提供者が提供するコンテンツ付加情報を格納し、コンテンツ付加情報抽出手段は、コンテンツ付加情報格納手段から、各利用者に応じたコンテンツ付加情報を抽出し、コンテンツ抽出手段は、コンテンツデータ格納手段から、選択されたコンテンツデータ及びコンテンツ鍵を抽出し、センタ秘密鍵復号手段は、コンテンツ抽出手段によって抽出されたコンテンツ鍵をセンタ秘密鍵により復号し、セッション鍵暗号化手段は、センタ秘密鍵復号手段によって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段によって抽出されたコンテンツ付加情報をセッション鍵によって暗号化し、情報配信手段は、コンテンツ抽出手段により抽出されたコンテンツデータ、及びセッション鍵暗号化手段により暗号化されたコンテンツ鍵及びコンテンツ付加情報を情報利用端末に配信する。

【００１７】また、コンテンツデータの保管及び配信を行う情報保管配信システムにおいて、送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、認証処理を行い、共有鍵であるセッション鍵を生成する認証手段と、前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、前記コンテンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する情報送信手段とを有する情報利用端末と、配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、前記配信コンテンツ選択手段による選択に応じて抽出され、前記コンテンツ鍵によって暗号化された前記コンテンツデータ、前記端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段とを有する情報利用端末と、前記情報利用端末との認証処理を行い、前記セッション鍵を生成する認証手段と、前記情報利用端末から送信された前記コンテン

ツデータ、前記コンテンツ鍵、及び前記コンテンツ情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、前記情報受信手段によって受信された前記コンテンツデータ、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格納手段と、前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、利用者の個人情報を格納する個人情報格納手段と、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信する情報配信手段とを有する情報保管配信装置とを有することを特徴とする情報保管配信システムが提供される。

【００１８】ここで、送信コンテンツ選択手段は、送信するコンテンツデータの選択を行い、コンテンツ鍵暗号化手段は、送信コンテンツ選択手段によって選択されたコンテンツデータをコンテンツ鍵によって暗号化し、端末秘密鍵暗号化手段は、端末秘密鍵によってコンテンツ鍵を暗号化し、認証手段は、認証処理を行い、共有鍵であるセッション鍵を生成し、セッション鍵暗号化手段は、端末秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を、セッション鍵により暗号化し、情報送信手段は、コンテンツ鍵暗号化手段によって暗号化されたコンテンツデータ、セッション鍵暗号化手段によって暗号化されたコンテンツ鍵、及びコンテンツデータの内容を示すコンテンツ情報を送信し、配信コンテンツ選択手段は、配信を希望するコンテンツの選択を行い、情報受信手段は、配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵により暗号化されたコンテンツ鍵、及びセッション鍵によって暗号化されたコンテンツ付加情報を受信し、セッション鍵復号手段は、セッション鍵により、情

報受信手段によって受信されたコンテンツ鍵及びコンテンツ付加情報を復号し、端末秘密鍵復号手段は、端末秘密鍵により、セッション鍵によって復号されたコンテンツ鍵を復号し、コンテンツ鍵復号手段は、端末秘密鍵復号手段によって復号されたコンテンツ鍵により、コンテンツデータを復号し、認証手段は、情報利用端末との認証処理を行い、セッション鍵を生成し、情報受信手段は、情報利用端末から送信されたコンテンツデータ、コンテンツ鍵、及びコンテンツ情報を受信し、セッション鍵復号手段は、情報受信手段によって受信されたコンテンツ鍵をセッション鍵により復号し、センタ秘密鍵暗号化手段は、セッション鍵復号手段により復号されたコンテンツ鍵をセンタ秘密鍵により暗号化し、コンテンツデータ格納手段は、情報受信手段によって受信されたコンテンツデータ、及びセンタ秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を格納し、コンテンツ情報格納手段は、情報受信手段によって受信されたコンテンツ情報を格納し、個人情報格納手段は、利用者の個人情報を格納し、コンテンツ付加情報格納手段は、付加情報提供者が提供するコンテンツ付加情報を格納し、コンテンツ付加情報抽出手段は、コンテンツ付加情報格納手段から、各利用者に応じたコンテンツ付加情報を抽出し、コンテンツ抽出手段は、コンテンツデータ格納手段から、選択されたコンテンツデータ及びコンテンツ鍵を抽出し、センタ秘密鍵復号手段は、コンテンツ抽出手段によって抽出されたコンテンツ鍵をセンタ秘密鍵により復号し、セッション鍵暗号化手段は、センタ秘密鍵復号手段によって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段によって抽出されたコンテンツ付加情報をセッション鍵によって暗号化し、情報配信手段は、コンテンツ抽出手段により抽出されたコンテンツデータ、及びセッション鍵暗号化手段により暗号化されたコンテンツ鍵及びコンテンツ付加情報を情報利用端末に配信する。

【００１９】さらに、送信するコンテンツデータの選択を行い、選択された前記コンテンツデータをコンテンツ鍵によって暗号化し、端末秘密鍵によって前記コンテンツ鍵を暗号化し、認証処理を行い、共有鍵であるセッション鍵を生成し、暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化し、暗号化された前記コンテンツデータ、前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する機能をコンピュータに行わせるプログラムを格納する記録媒体が提供される。

【００２０】また、認証処理を行い、共有鍵であるセッション鍵を生成し、配信を希望するコンテンツの選択を行い、利用者の選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によっ

て暗号化されたコンテンツ付加情報を受信し、受信された前記コンテンツ鍵及び前記コンテンツ付加情報を前記セッション鍵により復号し、前記セッション鍵によって復号された前記コンテンツ鍵を前記端末秘密鍵により復号し、復号された前記コンテンツ鍵により、前記コンテンツデータを復号する機能をコンピュータに行わせるプログラムを格納する記録媒体が提供される。

【００２１】さらに、認証処理を行い、共有鍵であるセッション鍵を生成し、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を受信し、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号し、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化し、受信した前記コンテンツデータ、及び暗号化された前記コンテンツ鍵を格納し、受信した前記コンテンツ情報を格納し、利用者の個人情報を格納し、付加情報提供者が提供するコンテンツ付加情報を格納し、各利用者に応じた前記コンテンツ付加情報を抽出し、利用者に選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出し、抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号し、復号された前記コンテンツ鍵、及び抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化し、抽出された前記コンテンツデータ、及び暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を配信する機能をコンピュータに行わせるプログラムを格納した記録媒体が提供される。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は、本形態における情報保管配信システム１の概略構成を示した構成図である。

【００２３】情報保管配信システム１は、コンテンツデータの利用を行う情報利用端末２、３、コンテンツデータの保管及び配信を行う情報保管配信装置４、及びコンテンツ付加情報の提供を行う付加情報提供者５によって構成されている。情報保管配信装置４は、利用者の個人情報を格納する個人情報格納手段４ａ、同じく情報利用端末２から送信されたコンテンツ情報を格納するコンテンツ情報格納手段４ｂ、コンテンツデータを格納するコンテンツデータ格納手段４ｃ、及び付加情報提供者５から提供された付加情報を格納するコンテンツ付加情報格納手段４ｄを有している。

【００２４】ここで、個人情報とは、本システムの利用者の個人情報であり、利用者の氏名、性別、住所、端末ＩＤ、クレジットカード番号、利用者が配信を希望する情報、配信を希望しない情報等が含まれる。また、コンテンツデータとは、音楽、映像等のデータであり、利用者は、インターネットからのダウンロード、ＣＤ等の購

入によりそれらの使用権を取得する。コンテンツデータは、デジタルデータとして扱い得るデータであり、データ送信時等にはコンテンツ鍵を用いて暗号化される。コンテンツ情報とは、コンテンツジャンル等のコンテンツデータの内容を示したデータ、及び利用者が設定した情報により構成され、例えば、コンテンツデータが音楽コンテンツの場合、音楽のタイトル、演奏者名、コンテンツ制作団体名等の情報が含まれる。コンテンツ付加情報とは、付加情報提供者５が提供するコンテンツに付加することを希望する情報、例えば、音楽コンテンツに関するものであれば、新譜情報、新譜ダウンロード先、演奏家情報、及びダウンロードサイト等の広告情報等であり、テキストデータの他、画像データ、音声データ等も含まれる。

【００２５】情報利用端末２は、本システムの利用者が使用権を取得したコンテンツを情報保管配信装置４に送信する装置であり、使用権を取得したコンテンツの保持を安全に行い、情報保管配信装置４とのコンテンツのやりとりを改竄、盗聴等の不正行為を防止しつつ行うことができる機能を有する。また、インターネットに接続する通信機能、及びＷｅｂページを表示する機能を有しており、これらにより、インターネットのダウンロードサイトからコンテンツの取得を行う。さらに、情報保管配信装置４へのコンテンツの送信処理を行うためのＧＵＩ（graphical user interface）ソフトウェアを有し、情報保管配信装置４が発行する本システム使用のための証明書を格納する記録装置を有している。

【００２６】情報利用端末３は、情報保管配信装置４から配信されたコンテンツを受信し、その利用を行う装置であり、情報保管配信装置４と接続するための移動体通信等の通信手段を有し、受信したコンテンツを格納する記憶装置、及びコンテンツ情報を表示する表示部を有している。

【００２７】情報保管配信装置４は、情報利用端末２から送信されたコンテンツ、及び付加情報提供者から送信されたコンテンツ付加情報を保管し、要求に応じて、保管されているコンテンツ及びコンテンツ付加情報を情報利用端末３に配信する装置である。

【００２８】付加情報提供者５は、コンテンツ付加情報の提供者であり、コンテンツのダウンロードサイト、コンテンツ所有者、コンテンツ制作者、企業、個人提供者等が含まれる。

【００２９】図２は、情報利用端末２の構成を示した構成図である。情報利用端末２は、使用権を取得したコンテンツデータを格納するコンテンツデータ格納手段２ａ、コンテンツデータ格納手段２ａに格納されたコンテンツのコンテンツ情報を格納するコンテンツ情報格納手段２ｂ、情報保管配信装置４に送信するコンテンツデータの選択を行う送信コンテンツ選択手段２ｃ、送信コンテンツ選択手段２ｃによって選択されたコンテンツデー

タをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段２ｄ、端末秘密鍵によってコンテンツ鍵を暗号化する端末秘密鍵暗号化手段２ｅ、情報保管配信装置４との認証処理を行い、情報保管配信装置４との共有鍵であるセッション鍵を生成する認証手段２ｆ、端末秘密鍵暗号化手段２ｅによって暗号化されたコンテンツ鍵を、セッション鍵により暗号化するセッション鍵暗号化手段２ｈ、コンテンツ鍵暗号化手段２ｄによって暗号化されたコンテンツデータ、セッション鍵暗号化手段２ｈによって暗号化されたコンテンツ鍵、コンテンツ情報、及び個人情報を情報保管配信装置４に送信する情報送信手段２ｉによって構成されている。

【００３０】ここで、コンテンツ鍵とは、コンテンツデータを暗号化及び復号する際に用いる鍵であり、暗号化されたコンテンツデータとともに情報保管配信装置４に送信される。端末秘密鍵とは、情報保管配信装置４への送信時にコンテンツ鍵を暗号化する際に用いる秘密鍵であり、情報利用端末２が有する図示していないモジュールに保持される。セッション鍵とは、後述する認証によって生成される情報利用端末２、３と情報保管配信装置４との共有鍵であり、端末秘密鍵によって暗号化されたコンテンツ鍵等をさらに暗号化及び復号するために用いる鍵である。

【００３１】図３は、情報利用端末３の構成を示した構成図である。情報利用端末３は、情報保管配信装置４との認証処理を行い、情報保管配信装置４との共有鍵であるセッション鍵を生成する認証手段３ａ、セッション鍵により暗号化され、情報保管配信装置４から送信されたコンテンツリストを受信するコンテンツリスト受信手段３ｂ、コンテンツリスト受信手段３ｂによって受信されたコンテンツリストをセッション鍵により復号するコンテンツリスト復号手段３ｃ、配信を希望するコンテンツの選択を行う配信コンテンツ選択手段３ｄ、配信コンテンツ選択手段３ｄによる選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵により暗号化されたコンテンツ鍵、及びセッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段３ｅ、情報受信手段３ｅによって受信されたコンテンツ鍵及びコンテンツ付加情報をセッション鍵により復号するセッション鍵復号手段３ｆ、端末秘密鍵により、セッション鍵によって復号されたコンテンツ鍵を復号する端末秘密鍵復号手段３ｇ、及び端末秘密鍵復号手段３ｇによって復号されたコンテンツ鍵により、コンテンツデータを復号するコンテンツ鍵復号手段３ｈによって構成されている。

【００３２】ここで、コンテンツリストとは、情報保管配信装置４のコンテンツデータ格納手段４ｃに格納されたコンテンツデータを示すリストであり、利用者はこのリストを参照し、配信を希望するコンテンツの選択を行う。

【００３３】図４は、情報保管配信装置４の構成を示した構成図である。情報保管配信装置４は、情報利用端末２、３との認証処理を行い、情報利用端末２、３との共有鍵であるセッション鍵を生成する認証手段４ｅ、コンテンツリストを作成するコンテンツリスト作成手段４ｎ、コンテンツデータ格納手段４ｃに格納されたコンテンツデータのリストであるコンテンツリストを、セッション鍵により暗号化するコンテンツリスト暗号化手段４ｏ、コンテンツリスト暗号化手段４ｏによって暗号化されたコンテンツリストを情報利用端末３に送信するコンテンツリスト送信手段４ｐ、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵によって暗号化されたコンテンツ鍵、及びコンテンツ情報を受信する情報受信手段４ｆ、セッション鍵により、情報受信手段４ｆによって受信されたコンテンツ鍵を復号するセッション鍵復号手段４ｇ、センタ秘密鍵によって、セッション鍵復号手段４ｇにより復号されたコンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段４ｈ、情報受信手段４ｆによって受信されたコンテンツデータ、及びセンタ秘密鍵暗号化手段４ｈによって暗号化されたコンテンツ鍵を格納するコンテンツデータ格納手段４ｃ、情報受信手段４ｆによって受信されたコンテンツ情報を格納するコンテンツ情報格納手段４ｂ、利用者の個人情報を格納する個人情報格納手段４ａ、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段４ｄ、コンテンツ付加情報格納手段４ｄから、各利用者に応じたコンテンツ付加情報を抽出するコンテンツ付加情報抽出手段４ｍ、コンテンツデータ格納手段４ｃから、選択されたコンテンツデータ及びコンテンツ鍵を抽出するコンテンツ抽出手段４ｉ、コンテンツ抽出手段４ｉによって抽出されたコンテンツ鍵をセンタ秘密鍵により復号するセンタ秘密鍵復号手段４ｊ、センタ秘密鍵復号手段４ｊによって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段４ｍによって抽出されたコンテンツ付加情報をセッション鍵によって暗号化するセッション鍵暗号化手段４ｋ、及び、コンテンツ抽出手段４ｉにより抽出されたコンテンツデータ、及びセッション鍵暗号化手段４ｋにより暗号化されたコンテンツ鍵及びコンテンツ付加情報を情報利用端末３に配信する情報配信手段４ｌによって構成されている。

【００３４】次に、本形態における情報保管配信システム１の動作について説明する。本システムは、利用者が事前に使用権を取得したコンテンツを情報保管配信装置４に送信・保管し、利用者がその保管したコンテンツを利用する際に、同時にコンテンツ付加情報の提供も受けられるというものである。以下、図１を用いて、情報保管配信システム１の概略動作について説明する。

【００３５】本システムの利用にあたり、まず利用者は

個人情報の登録を行う。個人情報の登録は、郵送、或いはインターネットのＷｅｂページ等により行い、登録された個人情報は、情報保管配信装置４の個人情報格納手段４ａに格納される。登録を行った利用者は、本システム提供者が発行する電子証明書を受け取り、受け取った電子証明書は、情報利用端末２、３が有する図示していないモジュールに格納される。

【００３６】個人情報の登録を行った利用者は、次に、利用者が使用権を取得しているコンテンツの送信を行う。コンテンツの使用権の取得は、インターネットからのダウンロード等によって事前に行われており、そのように取得されたコンテンツデータ及びコンテンツ情報は情報利用端末２に格納されている。利用者は、このように情報利用端末２に格納されているコンテンツデータ及びコンテンツ情報を情報保管配信装置４に暗号化して送信し、情報保管配信装置４は、送信されたコンテンツデータをコンテンツデータ格納手段４ｃに、コンテンツ情報をコンテンツ情報格納手段４ｂにそれぞれ格納する。

【００３７】また、付加情報提供者５は、各種のコンテンツ付加情報を情報保管配信装置４に送信し、コンテンツ付加情報を受け取った情報保管配信装置４は、受け取ったコンテンツ付加情報をコンテンツ付加情報格納手段４ｄに格納する。

【００３８】利用者が情報保管配信装置４に送信したコンテンツを利用しようとする場合、まず利用者は、情報利用端末３を用いて情報保管配信装置４に接続し、情報保管配信装置４から送られるコンテンツデータ格納手段４ｃに格納されている自己のコンテンツデータのリストであるコンテンツリストを取得する。コンテンツリストを取得した利用者は、そのコンテンツリストを参照し、利用を希望するコンテンツを選択し、情報保管配信装置４からそのコンテンツデータの配信を受ける。この際、情報保管配信装置４は、利用者の個人情報及びコンテンツ情報等を参照し、その利用者に適したコンテンツ付加情報を抽出し、コンテンツデータとともに利用者に配信する。このようにすることにより、コンテンツデータの配信時に利用者に適した情報を自動的に提供することが可能となる。

【００３９】次に、情報利用端末２、３と情報保管配信装置４での情報のやりとりについて説明する。まず、情報利用端末２から情報保管配信装置４へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置４への保管処理について説明する。図５及び図６は、これらの過程の動作手順を示した図である。

【００４０】まず、情報利用端末２において送信ＧＵＩソフトウェアを起動し、情報利用端末２に格納されているコンテンツデータのリストを表示する。利用者は、表示されたリストを参照し、配信を希望するコンテンツデータ及びそのコンテンツ情報を選択する。選択されたコンテンツデータは、コンテンツ鍵により暗号化され、この暗号化に用いられたコンテンツ鍵は、端末秘密鍵により暗号化される。

【００４１】次に、情報利用端末２は情報保管配信装置４との認証処理を行い、セッション鍵の生成が行われる。セッション鍵の生成が終了すると、情報利用端末２は、そのセッション鍵を用い、選択されたコンテンツ情報、及び端末秘密鍵により暗号化されたコンテンツ鍵を暗号化する。そして、このように暗号化されたコンテンツ情報、コンテンツ鍵、及びコンテンツ鍵により暗号化されたコンテンツデータは、情報保管配信装置４に送信される。

【００４２】情報利用端末２から送信されたコンテンツ情報及びコンテンツデータは、情報保管配信装置４に受信され、情報保管配信装置４のコンテンツデータ格納手段４ｃに格納される。一方、受信されたコンテンツ鍵は、セッション鍵によって復号され、次に、センタ秘密鍵により暗号化された後格納される。これらの情報の格納が終了すると、情報保管配信装置４は、情報の送信が完了した旨の信号を情報利用端末２に送る。

【００４３】次に、コンテンツの配信動作について説明する。図７は、この過程の動作手順を示した図である。利用者が情報保管配信装置４に格納したコンテンツの配信を希望する場合、利用者は、まず、情報保管配信装置４との認証処理を行い、セッション鍵を生成する。セッション鍵が生成されると、情報保管配信装置４は、格納しているコンテンツのリストであるコンテンツリストを作成する。作成されたコンテンツリストは、セッション鍵によって暗号化され、暗号化されたコンテンツリストは情報利用端末３に送信される。

【００４４】このように送信されたコンテンツリストは、情報利用端末３によって受信され、セッション鍵によって復号される。利用者は、復号されたコンテンツリストを参照して配信を希望するコンテンツの選択を行い、配送を希望するコンテンツの指定を行う。

【００４５】コンテンツの指定は、情報保管配信装置４に伝えられ、情報保管配信装置４は、指定されたコンテンツデータ及びそのコンテンツ鍵をコンテンツデータ格納手段４ｃから抽出し、それに加え、利用者に適したコンテンツ付加情報をコンテンツ付加情報格納手段４ｄから抽出する。

【００４６】このように抽出されたコンテンツ鍵、及びコンテンツ付加情報は、セッション鍵で暗号化され、コンテンツ鍵で暗号化されているコンテンツデータとともに情報利用端末３に配信される。情報利用端末３に配信されたコンテンツ鍵、コンテンツ付加情報及びコンテンツデータは、情報利用端末３によって受信され、これらを受信した情報利用端末３は、情報保管配信装置４に、配信が完了した旨の信号を送信する。

【００４７】情報利用端末３によって配信されたコンテンツ鍵及びコンテンツ付加情報はセッション鍵で復号さ

れ、さらにコンテンツ鍵は端末秘密鍵で復号される。そして、情報利用端末３は、復号されたコンテンツ鍵を用い、コンテンツデータを復号し、復号したコンテンツデータ及びコンテンツ付加情報を格納する。

【００４８】次に、図２から図４を用い、情報保管配信システム１の詳細動作について説明する。まず、情報利用端末２から情報保管配信装置４へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置４への保管処理について説明する。なお、以下の説明では、既に利用者の個人情報の登録は終了し、その個人情報は情報保管配信装置４の個人情報格納手段４ａに格納されており、また、情報利用端末２のコンテンツデータ格納手段２ａには利用者が使用権を取得したコンテンツデータが、コンテンツ情報格納手段２ｂにはそのコンテンツ情報がそれぞれ格納されているものとする。

【００４９】まず、利用者は情報利用端末２が有するＧＵＩソフトウェアを起動し、コンテンツデータ格納手段２ａに格納されているコンテンツデータのリストを表示する。利用者は、表示されたリストを参照し、送信コンテンツ選択手段２ｃを用いて、配信を希望するコンテンツを指定する。送信コンテンツ選択手段２ｃは、利用者からの指定に従い、情報保管配信装置４に送信するコンテンツデータ及びそのコンテンツ情報をコンテンツデータ格納手段２ａ及びコンテンツ情報格納手段２ｂから抽出する。抽出されたコンテンツデータは、コンテンツ鍵暗号化手段２ｄにおいてコンテンツ鍵により暗号化され、この暗号化に用いられたコンテンツ鍵は、端末秘密鍵暗号化手段２ｅにおいて端末秘密鍵により暗号化される。

【００５０】次に、認証手段２ｆにおいて、登録により取得した電子証明書を用い、情報保管配信装置４の認証手段４ｅとの認証処理を行う。この認証処理は、後述するＡＫＥ　Ｐｒｏｔｏｃｏｌ等を利用して行い、この認証処理の後、セッション鍵の生成が行われる。

【００５１】セッション鍵の生成が終了すると、セッション鍵暗号化手段２ｈは、そのセッション鍵を用い、送信コンテンツ選択手段２ｃによって抽出されたコンテンツ情報、及び端末秘密鍵暗号化手段２ｅにおいて暗号化されたコンテンツ鍵を暗号化する。そして、セッション鍵暗号化手段２ｈにおいて暗号化されたコンテンツ情報、コンテンツ鍵、及びコンテンツ鍵暗号化手段２ｄにおいて暗号化されたコンテンツデータは、情報送信手段２ｉにより情報保管配信装置４に送信される。

【００５２】情報利用端末２から送信されたコンテンツ情報、コンテンツ鍵及びコンテンツデータは、情報受信手段４ｆによって受信され、受信されたコンテンツ情報はコンテンツ情報格納手段４ｂに、コンテンツデータはコンテンツデータ格納手段４ｃにそれぞれ格納される。一方、受信されたコンテンツ鍵は、セッション鍵復号手段４ｇにおいてセッション鍵を用いて復号され、次に、

センタ秘密鍵暗号化手段４ｈにおいてセンタ秘密鍵により暗号化された後、コンテンツデータ格納手段４ｃに格納される。これにより、情報保管配信装置４に格納されたコンテンツを利用者等が不正に引き出すことを防止することができる。

【００５３】なお、情報利用端末２は、ＧＵＩソフトウェアを用い、配信されるコンテンツの種類、順番等をエディットしたパッケージ情報を設定することが可能であり、コンテンツの送信時にこのパッケージ情報を送信することもできる。このように、送信されたパッケージ情報は、情報保管配信装置４のコンテンツ情報格納手段４ｂに格納される。

【００５４】次に、付加情報提供者５によるコンテンツ付加情報の登録について説明する。付加情報提供者５は、情報保管配信システム１へのコンテンツ付加情報の提供にあたり、まず決済方法、契約条件等の登録を行う。登録は、郵送、或いはインターネットのＷｅｂページ等を用いて行われ、登録を行った付加情報提供者５は、情報保管配信装置４のＷｅｂサイトにアクセスするためのユーザＩＤ、パスワード等を取得する。

【００５５】登録を終了した付加情報提供者５がコンテンツ付加情報の提供を希望する場合、付加情報提供者５は、取得したユーザＩＤ及びパスワードを用いて情報保管配信装置４のＷｅｂサイトにアクセスし、コンテンツ付加情報の送信を行う。このように送信されたコンテンツ付加情報は、情報保管配信装置４のコンテンツ付加情報格納手段４ｄに格納される。情報格納手段４ｄに格納されたコンテンツ付加情報は、付加情報提供者５の希望に応じて随時更新、変更され、情報格納手段４ｄには、常に最新の情報が保持される。

【００５６】次に、コンテンツの配信動作について説明する。利用者が情報保管配信装置４に格納したコンテンツの配信を希望する場合、利用者は、電子証明書を用い、情報利用端末３の認証手段３ａによって、情報保管配信装置４の認証手段４ｅとの認証処理を行う。この認証処理は、後述するＡＫＥ　Ｐｒｏｔｏｃｏｌ等を利用して行い、この認証処理の後、セッション鍵の生成が行われる。

【００５７】セッション鍵が生成されると、情報保管配信装置４のコンテンツリスト作成手段４ｎは、コンテンツ情報格納手段４ｂに格納されたコンテンツ情報を用い、格納しているコンテンツのリストであるコンテンツリストを作成する。作成されたコンテンツリストは、コンテンツリスト暗号化手段４ｏによって暗号化され、暗号化されたコンテンツリストはコンテンツリスト送信手段４ｐによって情報利用端末３に送信される。なお、上述したパッケージ情報が作成されている場合には、コンテンツリストとともに、このパッケージ情報も送信されることとしてもよい。

【００５８】このように送信されたコンテンツリスト等

は、情報利用端末３のコンテンツリスト受信手段３ｂによって受信され、受信されたコンテンツリスト等は、コンテンツリスト復号手段３ｃによって復号される。利用者は、復号されたコンテンツリストを参照して配信を希望するコンテンツの選択を行い、配信コンテンツ選択手段３ｄを用いて、配送を希望するコンテンツの指定を行う。配信コンテンツ選択手段３ｄによるコンテンツの指定は、情報保管配信装置４のコンテンツ抽出手段４ｉに伝えられ、コンテンツ抽出手段４ｉは、コンテンツデータ格納手段４ｃから指定されたコンテンツデータ及びそのコンテンツ鍵を抽出し、抽出されたコンテンツ鍵は、センタ秘密鍵復号手段４ｊによって復号される。

【００５９】一方、コンテンツ付加情報抽出手段４ｍは、個人情報格納手段４ａ及びコンテンツ情報格納手段４ｂを元に、利用者に適したコンテンツ付加情報をコンテンツ付加情報格納手段４ｄから抽出する。

【００６０】このようにセンタ秘密鍵復号手段４ｊによって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段４ｍによって抽出されたコンテンツ付加情報は、セッション鍵暗号化手段４ｋにおいてセッション鍵で暗号化される。このようにセッション鍵で暗号化されたコンテンツ鍵及びコンテンツ付加情報は、コンテンツ鍵で暗号化されているコンテンツデータとともに、情報配信手段４ｌによって情報利用端末３に配信される。

【００６１】配信されたコンテンツ鍵、コンテンツ付加情報及びコンテンツデータは、情報利用端末３の情報受信手段３ｅによって受信され、これらを受信した情報利用端末３は、情報保管配信装置４に、配信が完了した旨のメッセージを送信する。情報保管配信装置４は、このメッセージを受け取ると、配信したコンテンツの情報等を使用履歴として残し、その使用履歴を課金処理、マーケティング情報等に利用する。

【００６２】一方、情報受信手段３ｅによって配信されたコンテンツ鍵及びコンテンツ付加情報は、セッション鍵復号手段３ｆにおいて、セッション鍵で復号され、また、セッション鍵復号手段３ｆによって復号されたコンテンツ鍵は、さらに端末秘密鍵復号手段３ｇにおいて、端末秘密鍵で復号される。そして、コンテンツ鍵復号手段３ｈは、端末秘密鍵復号手段３ｇで復号されたコンテンツ鍵を用い、コンテンツデータを復号する。

【００６３】以上のように復号されたコンテンツ付加情報、コンテンツ鍵及びコンテンツデータは、図示していない情報利用端末３の記録装置に格納され、これらのデータによってコンテンツ及びコンテンツ付加情報の表示等が行われる。

【００６４】図８は、ＡＫＥ　Ｐｒｏｔｏｃｏｌを用いた認証処理の様子を示した図である。この図において、E_{center}とは、情報保管配信装置４側のセンタ公開鍵e_{center}を用いた暗号化関数であり、E_{user}とは、電子証明書に含まれる端末公開鍵e_{user}を用いた暗号化関数で

あり、D_{center}とは、情報保管配信装置４側のセンタ秘密鍵d_{center}を用いた復号化関数であり、D_{user}とは、端末側秘密鍵d_{user}を用いた復号化関数である。情報利用端末２は、端末側秘密鍵d_{user}及び端末公開鍵e_{user}を有しており、登録時にセンタ公開鍵e_{center}を取得する。一方、情報保管配信装置４は、センタ公開鍵e_{center}、センタ秘密鍵d_{center}及び端末公開鍵e_{user}を有している。

【００６５】まず、情報利用端末２は、乱数ｒ１を生成し、e_{center}を用いてｒ１を暗号化し（$C1=E_{center}(r1)$を生成する）、Ｃ１を情報保管配信装置４に送る。情報保管配信装置４は、d_{center}を用いてＣ１を復号する（$t1=D_{center}(C1)$を生成する）。また、情報保管配信装置４は、乱数ｒ２を生成し、e_{user}を用いてｒ２を暗号化し（$C2=E_{user}(r2)$を生成する）、ｔ１とＣ２を情報利用端末２に送る。

【００６６】情報利用端末２は、ｔ１＝ｒ１であるか否かを判断し、ｔ１＝ｒ１である場合、d_{user}を用いてＣ２を復号し（$t2=D_{user}(C2)$を生成する）、ｔ２を情報保管配信装置４に送る。

【００６７】情報保管配信装置４では、ｔ２＝ｒ２であるか否か判断し、ｔ２＝ｒ２である場合、セッション鍵Ｋを生成し、e_{user}を用いてＫを暗号化する（$S=E_{user}(K)$を生成する）。Ｓは情報利用端末２に送られる。

【００６８】情報利用端末２は、d_{user}を用いてＳを復号する（$K=D_{user}(S)$を生成する）。その後、情報利用端末２と情報保管配信装置４との情報のやりとりには、このセッション鍵が使用される。

【００６９】なお、以上の説明では、情報利用端末２と情報保管配信装置４との認証処理について説明したが、情報利用端末３と情報保管配信装置４との認証処理も同様な手順によって行われる。

【００７０】このように、本形態では、利用者が使用権を取得したコンテンツを、情報利用端末２を用いて情報保管配信装置４に送信し、情報保管配信装置４は、そのコンテンツを保管し、利用者が情報保管配信装置４に格納されたコンテンツの利用を希望する場合、利用者は情報利用端末３を用いて情報保管配信装置４に格納されたコンテンツの配信を要求し、情報保管配信装置４は、要求されたコンテンツを情報利用端末３に配信することとしたため、利用者は、利用者が所持する記録装置の記憶容量に制限されることなく、コンテンツを保有することが可能となる。

【００７１】また、コンテンツは情報保管配信装置４に格納され、コンテンツの管理は、情報保管配信装置４によって行われることとしたため、管理上の利便性が高まり、再生時におけるコンテンツの選択が容易になる。

【００７２】さらに、コンテンツは情報保管配信装置４に格納され、利用者は、情報利用端末３を用い、情報保

管配信装置４から配信されたコンテンツを利用することとしたため、記録媒体を所持していない状況下であってもコンテンツの再生が可能となる。

【００７３】また、コンテンツの再生のために記録媒体を用いないため、情報利用端末３は、記録媒体の収納スペース、及び記録媒体再生のための駆動部を設ける必要がなくなり、情報利用端末３の小型化を図ることが可能となる。

【００７４】さらに、情報保管配信装置４は、情報利用端末３にコンテンツの配信を行う際、利用者の適した個人向け情報であるコンテンツ付加情報を送信することとしたため、各利用者は、自己が必要とする情報を自動的に入手することが可能となる。

【００７５】なお、上記の処理機能は、コンピュータによって実現することができる。その場合、情報利用端末２、３及び情報保管配信装置４が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておく。そして、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場に流通させる場合には、ＣＤ－ＲＯＭ(Compact Disk Read Only Memory)やフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。ここでコンピュータとは、特にパーソナルコンピュータには限定されず、少なくとも１つの処理装置を有し、プログラムによって制御されるコンピュータ一般を意味する。

【００７６】また、本形態では、情報利用端末２と情報利用端末３を別々に構成することとしたが、情報利用端末２と情報利用端末３とを一体化する構成としてもよい。

【００７７】

【発明の効果】以上説明したように本発明の情報利用端末では、使用権を取得したコンテンツを情報保管配信装置に送信することとしたため、使用権を取得したコンテンツを制限なく保有することができ、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、装置の小型化を図ることが可能となる。

【００７８】また、本発明の情報利用端末では、情報保管配信装置に記録しておいた使用権を取得したコンテンツを選択し、情報保管配信装置から配信されたコンテンツを利用することとしたため、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【００７９】さらに、本発明の情報保管配信装置では、情報利用装置から送信されたコンテンツを保管し、利用者からの要求に応じて格納したコンテンツを抽出し、抽出したコンテンツをコンテンツ付加情報とともに情報利用端末に配信することとしたため、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【００８０】また、本発明の情報保管配信システムでは、情報利用端末によって、使用権を取得したコンテンツを情報保管配信装置に送信し、情報保管配信装置によって、情報利用装置から送信されたコンテンツを保管し、利用者からの要求に応じて格納したコンテンツを抽出し、抽出したコンテンツをコンテンツ付加情報とともに情報利用端末に配信し、情報利用端末によって、情報保管配信装置に記録しておいた使用権を取得したコンテンツを選択し、情報保管配信装置から配信されたコンテンツを利用することとしたため、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【００８１】さらに本発明の記録媒体に格納されたプログラムをコンピュータ上で実行させることにより、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【図面の簡単な説明】

【図１】情報保管配信システムの概略構成を示した構成図である。

【図２】情報利用端末の構成を示した構成図である。

【図３】情報利用端末の構成を示した構成図である。

【図４】情報保管配信装置の構成を示した構成図である。

【図５】情報利用端末から情報保管配信装置へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置への保管処理における動作手順を示した図である。

【図６】情報利用端末から情報保管配信装置へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置への保管処理における動作手順を示した図である。

25

【図７】コンテンツの配信動作手順を示した図である。

【図８】ＡＫＥ　Ｐｒｏｔｏｃｏｌを用いた認証処理の様子を示した図である。

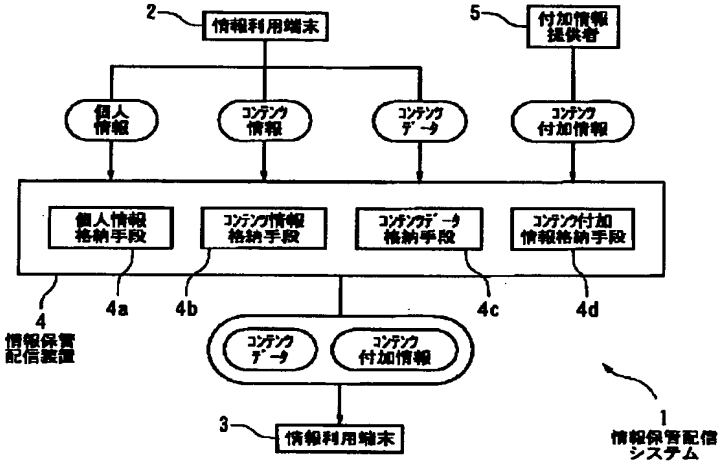
【符号の説明】

１…情報保管配信システム、２、３…情報利用端末、２ａ…コンテンツデータ格納手段、２ｂ…コンテンツ情報格納手段、２ｃ…送信コンテンツ選択手段、２ｄ…コンテンツ鍵暗号化手段、２ｅ…端末秘密鍵暗号化手段、２ｆ、３ａ、４ｅ…認証手段、２ｈ…セッション鍵暗号化手段、２ｉ…情報送信手段、３ｂ…コンテンツリスト受信手段、３ｃ…コンテンツリスト復号手段、３ｄ…配信コンテンツ選択手段、３ｅ…情報受信手段、３ｆ…セッ*

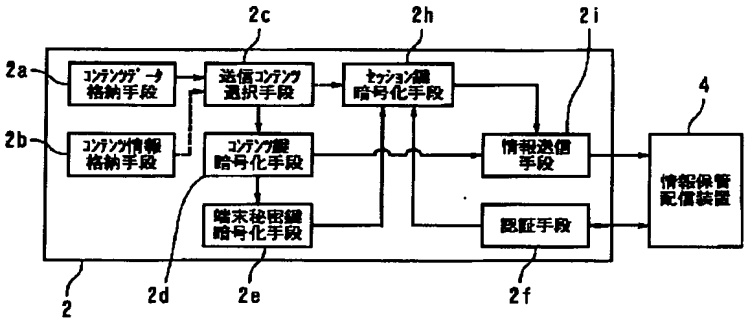
26

*ション鍵復号手段、３ｇ…端末秘密鍵復号手段、３ｈ…コンテンツ鍵復号手段、４ａ…個人情報格納手段、４ｂ…コンテンツ情報格納手段、４ｃ…コンテンツデータ格納手段、４ｄ…コンテンツ付加情報格納手段、４ｆ…情報受信手段、４ｇ…セッション鍵復号手段、４ｈ…センタ秘密鍵暗号化手段、４ｉ…コンテンツ抽出手段、４ｊ…センタ秘密鍵復号手段、４ｋ…セッション鍵暗号化手段、４ｌ…情報配信手段、４ｍ…コンテンツ付加情報抽出手段、４ｎ…コンテンツリスト作成手段、４ｏ…コンテンツリスト暗号化手段、４ｐ…コンテンツリスト送信手段

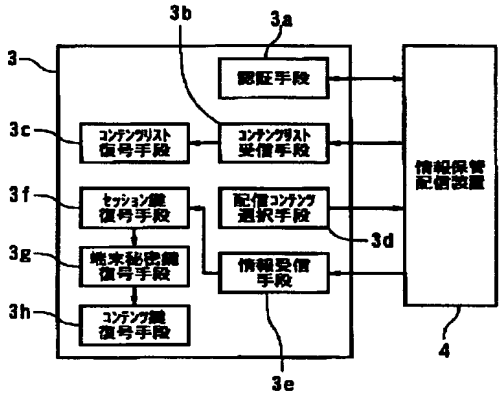
【図１】



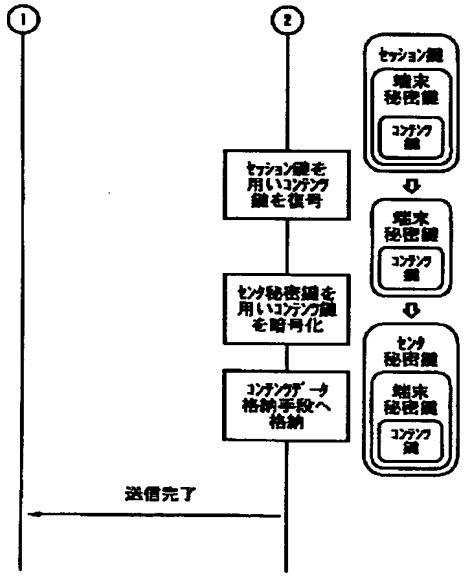
【図２】



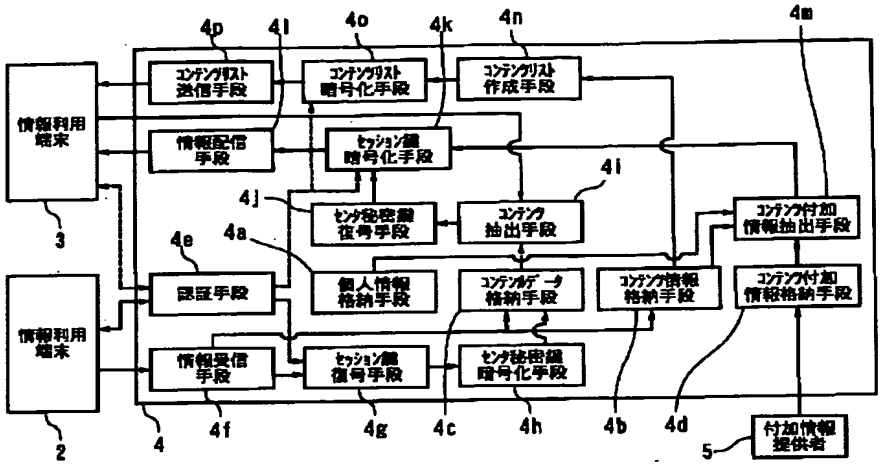
【図３】



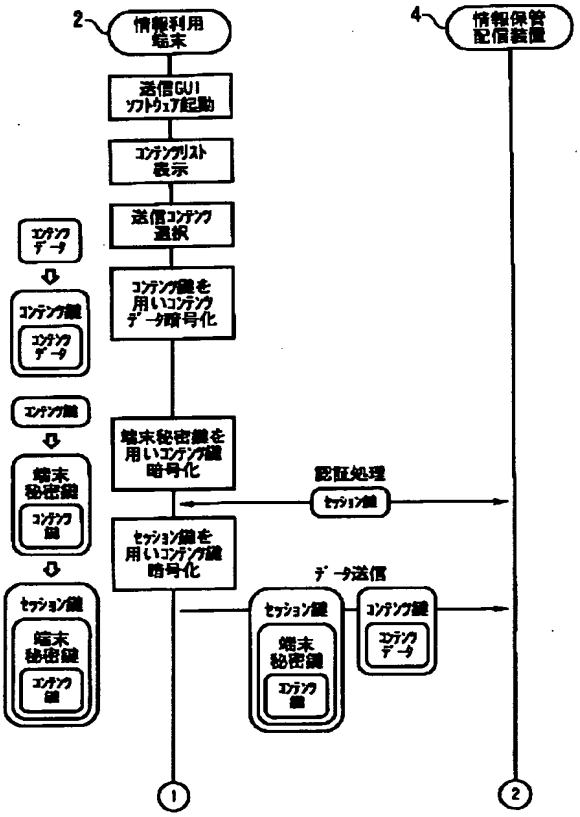
【図６】



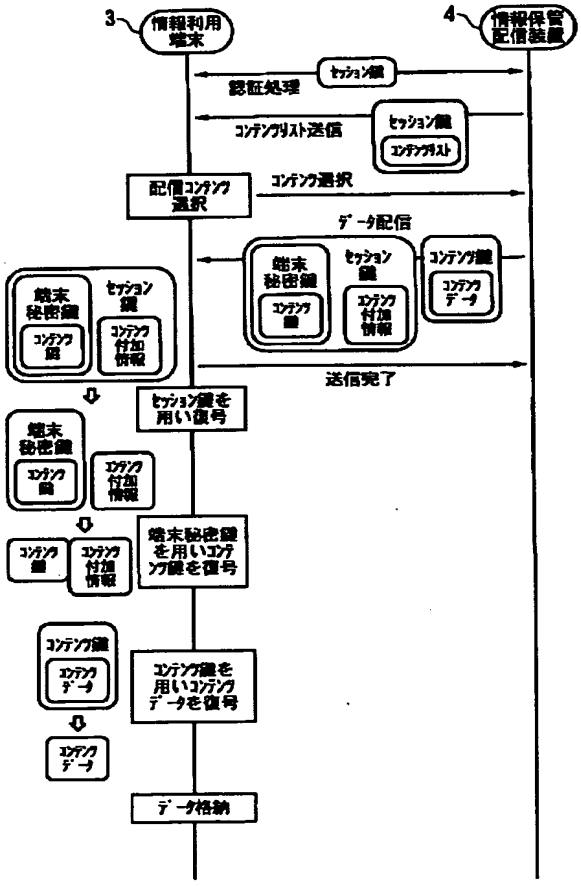
【図４】


情報利用端末
情報利用端末
コンテンツリスト送信手段
コンテンツリスト暗号化手段
コンテンツリスト作成手段
情報配信手段
セッション鍵暗号化手段
センタ秘密鍵復号手段
コンテンツ抽出手段
コンテンツ付加情報抽出手段
認証手段
個人情報格納手段
コンテンツデータ格納手段
コンテンツ情報格納手段
コンテンツ付加情報格納手段
情報受信手段
セッション鍵復号手段
センタ秘密鍵暗号化手段
付加情報提供者
3
2
4
4f
4g
4c
4h
4b
4d
5
4p
4l
4o
4k
4n
4m
4j
4i
4e
4a

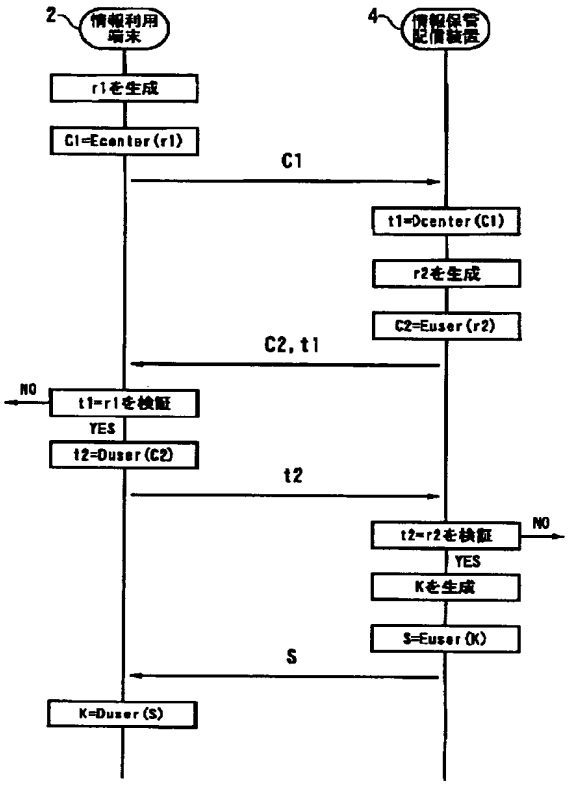
【図５】


2
情報利用端末
4
情報保管配信装置
送信GUIソフトウェア起動
コンテンツリスト表示
送信コンテンツ選択
コンテンツ鍵を用いコンテンツデータ暗号化
端末秘密鍵を用いコンテンツ鍵暗号化
認証処理
セッション鍵
セッション鍵を用いコンテンツ鍵暗号化
データ送信
コンテンツデータ
コンテンツ鍵
端末秘密鍵
セッション鍵
①
②

【図７】


3
情報利用端末
4
情報保管配信装置
認証処理
セッション鍵
コンテンツリスト送信
コンテンツリスト
配信コンテンツ選択
コンテンツ選択
データ配信
端末秘密鍵
コンテンツ鍵
コンテンツ付加情報
コンテンツデータ
送信完了
セッション鍵を用い復号
端末秘密鍵を用いコンテンツ鍵を復号
コンテンツ鍵を用いコンテンツデータを復号
データ格納

【図８】



フロントページの続き

(51) Int. Cl.[7]	識別記号	FI	テーマコード(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ　５Ｊ１０４
9/32			６０１Ｅ
			６７３Ｂ

Ｆターム(参考)　5B017 AA07 BA07 CA16
5B049 AA01 BB00 EE05 FF07 GG02
GG10
5B082 EA11 HA05
5B085 AE29
5B089 GA21 GB04 HA10 JA33 JB22
KA11 KA13 KA17 KB04 KB13
KC58 KH30 LB01 LB14
5J104 AA01 AA07 AA16 EA04 EA07
EA18 EA19 JA03 KA02 NA03
NA27 PA07